一种实用的轻量级RFID安全协议研究

姜丽芬[1] 李章林[2] 辛运帏[2]
(天津师范大学计算机与信息工程学院 天津 300074)[1]
(南开大学机器人与信息自动化研究所 天津 300071)[2]

摘 要 RFID的安全问题是RFID应用中的关键问题之一。RFID标签计算资源有限,因此旨在研究一种轻量级且具有一定安全性的RFID安全协议,使得标签端的协议不包含复杂的加密操作,只包含异或和简单逻辑控制。证明了"RFID标签最小限度密码算法"存在弱点,并针对该弱点提出了信道加密等3点改进方法,改进后攻击者不能直接计算密码而需强力攻击。实验结果表明,改进后,破解所需时间和所需记录数都增加,且破解难度随着信道密码长度的增加呈指数增加而加密复杂度呈线性增加。另外改进后对硬件需求的增加不多。该协议有助于在低成本RFID标签上实现较高安全性的RFID安全协议。

关键词 RFID,安全,隐私,轻量级

Research of a Practical Lightweight RFID Security Protocol

JIANG Li-fen[1] LI Zhang-lin[2] XIN Yun-wei[2]
(College of Computer and Information Engineering, Tianjin Normal University, Tianjin 300074, China)[1]
(Institute of Robotics and Information Automatic System, Nankai University, Tianjin 300071, China)[2]

Abstract RFID security is a key issue in RFID application. According to limited computational resources of RFID tags, we aimed to design a lightweight RFID security protocol with appropriate security, which has no complicated cryptographic operations in the tag side, but only XOR and simple logical control. The paper proved that there is weakness in "Minimalist Cryptography for Low-Cost RFID Tags", and according to this weakness, the paper promoted three methods, including channel encryption. Attackers can't compute the key directly with the improved protocol, but must resort to brute-force search. The experimental result showed that the cracking time and the record number needed for cracking increased with improved protocol, and the cracking difficulty increases exponentially when the length of channel key increases, but the encryption complication increases in linear. Furthermore, the hardware requirement doesn't increase much. The protocol helps to realize relatively high security in low-cost RFID tags.

Keywords RFID, Security, Privacy, Lightweight

1 引言

无线射频识别(Radio Frequency Identification, RFID)技术,是一种利用射频通信实现的非接触式自动识别技术。RFID系统一般由3大部分构成:RFID标签(后面简称标签)、RFID标签读写器(后面简称读写器)和后端数据库。标签在靠近读写器时,通过读写器发出的电磁波获得能量,并给读写器发送标签ID。由于标签具有体积小、相对条形码容量较大、可支持非可视识别等优点,在物流、公共安全、交通管理等领域有广阔的应用前景。

但是RFID的广泛应用将引起安全和隐私问题。RFID的安全威胁主要是攻击者可以监听标签和读写器的交互数据以及任何读写器都可读取标签的内容。A. Juels[1]认为RFID的安全问题包括隐私问题和认证问题。隐私问题是由读写器读标签时无需认证引起,包括跟踪问题和泄露信息问题;认证问题是由标签被读取时无需认证引起,包括标签克隆、篡改标签数据等。RFID的安全问题渐渐受到重视,中国射频识别技术政策白皮书[2]指出RFID的共性和前瞻性技术包括安全算法和实现技术。而国内RFID安全研究才处于起步阶段。

RFID安全问题的特殊性在于标签的计算能力有限。典型的标签的电流只有15mA,门阵列只有5000个[3],这使得在安全领域的很多通用算法和协议不能够在标签上实现,例如一个商业用途的AES对称加密算法大概需要20,000～30,000个门电路[4]。虽然摩尔定律认为芯片的集成度会快速增加,但是对于使用量巨大的RFID芯片,追求低成本是它的设计目标。RFID的安全问题给研究者提出了挑战,研究轻量级的RFID安全协议成为其中的热点。

A. Jules[1]根据标签的计算资源将RFID标签分为3类:

1)基本标签:指那些不能够执行标准的加密操作(比如产生随机码、执行杂凑(hash)函数等)的标签,但可以有异或(XOR)操作和简单的逻辑控制。

2)对称密码标签:指能够执行对称密码加密操作的标签。

到稿日期:2008-12-04 返修日期:2009-03-31 本课题受天津市自然科学基金项目(06YFJMJC00200)资助。
姜丽芬 女,副教授,博士,E-mail:jianglf@robot.nankai.edu.cn;李章林 男,博士;辛运帏 女,教授,博士。

3)公钥密码标签:指能够执行公钥加密的标签。

事实上,该分类也将 RFID 安全协议按顺序分为三类协议。实现第三类安全协议的一般是主动式标签(Active Tag),例如用于集装箱的主动标签、高安全非接触卡。再次加密机制(Re-encryption)[5]虽然也使用公钥,但它的加密、解密算法不在标签上执行,而是将加密的结果写入标签作为 ID,只有持有私钥的读写器能够从 ID 解密得到明文。该协议应该属于第一类协议。

杂凑函数是实现第二类安全协议的重要方法[6-9]。设 h 为杂凑函数,则标签用发送$(r,h(ID,r))$代替发送 ID,由于杂凑函数的不可逆性攻击者从 $h(ID,r)$无法计算 ID,从而保护隐私,随机数 r 使得发送数据每次不同,从而防止跟踪。另外还可以进一步加入随机挑战(challenge -response)机制来防止重放(Replay)攻击。该类方法需要在标签上实现杂凑函数甚至随机数产生器。

文献[10]认为 RFID 安全机制的方法主要有三大类:物理方法、密码机制以及二者的结合。本文将物理方法如"Kill 命令机制"、"静电屏蔽"、"主动干扰"、"Blocker Tag"等方法[1]视为第一类安全协议。第二类安全协议的另一种形式是采用异或和简单的逻辑控制,该类协议目前主要是 A. Juels 等人提出的最低限度密码算法(Minimalist Cryptography)[11]。该类协议对硬件需求小,适合在 RFID 上实现。需要指出的是由于读写器计算能力较强,允许读写器端的协议进行复杂的加密操作。本文以最低限度密码算法为基础提出了改进算法,显著提高了安全性,并只增加少量硬件开销。

2 RFID 最小限度密码算法的问题及改进

2.1 RFID 最小限度算法简介

A. Jues 等人的 RFID 最小限度密码算法描述的标签和读写器的一次交互过程如图 1 所示。标签和读写器共享(共享指双方各有一套,且完全相同)三种密码:α,β,γ(按顺序分别为第 1,2,3 种密码),每种密码有 k 个,密码长度都为 l 比特。每个标签都有一套该密码,密码在标签之间互相保密,但读写器有所有标签的密码(例如所有标签的密码存于后端数据库中)。

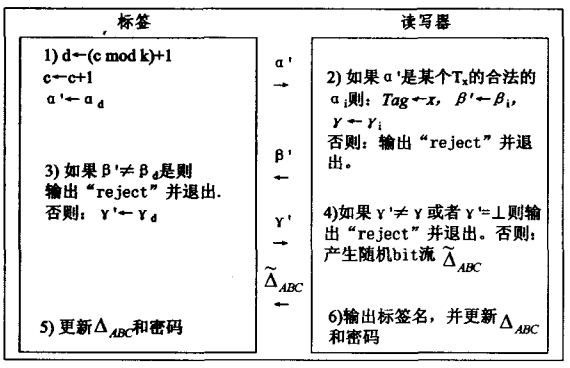

图 1 最低限度密码算法

1)首先,标签选择 k 个 α 中的第 d 个作为 α'并发送给读写器。d 为此次交互使用的密码序号。d 的更新方法如图 1 所示,每 k 次交互后 d 回到原值。

2)读写器收到 α'后在数据库中搜索所有标签的 α。若标签 T_x 的第 i 个密码值 α_i 等于 α',可以基本确定标签名为 T_x,并令 α_i 对应(所谓对应指密码序号相同)的 β_i 为 β',α_i 对应的 γ_i 为 γ。接着读写器发送 β'。

3)标签根据 β'判断读写器的合法性,因为只有合法的读写器才能给出 α'对应的 β'。验证后标签发送 α'对应的 γ'。

4)读写器通过验证 γ'是否等于 γ 来最终验证标签的合法性,因为只有合法的标签才能给出 α'对应的 γ'。然后,读写器产生 3mk 个 l 比特的随机数组成的 bit 流 $\tilde{\Delta}_{ABC}$,并发送给标签,其中 m 是常数。

5)和 6):标签和读写器同步更新 Δ_{ABC} 和密码。Δ_{ABC} 是标签和读写器共享的 3mk 个 l 比特的数组成的 bit 流。

该算法通过标签和读写器共享的密码进行双向验证,即标签验证读写器,读写器也验证标签。读写器对 α'给出 β',标签对 β'给出 γ,这种 α',β',γ 的交互是一种随机挑战,可防止重放攻击。每次交互后的密码更新可防止跟踪。

2.2 最小限度算法存在的问题

下面证明攻击者通过连续监听多次交互数据可破解该协议。所谓破解这里指攻击者可以预知下次交互的 α',β',γ。该协议的弱点在密码更新方法,首先介绍该更新方法。将以上 3mk 个 l 比特数分解,设第 j 次交互的 Δ_{ABC} 和 $\tilde{\Delta}_{ABC}$ 为:

$$\Delta_{j,ABC}=(\Delta_{j,1,1},\Delta_{j,1,2},\cdots,\Delta_{j,1,k},\Delta_{j,2,1},\Delta_{j,2,2},\cdots,\Delta_{j,3,k})$$
$$\tilde{\Delta}_{j,ABC}=(\tilde{\Delta}_{j,1,1},\tilde{\Delta}_{j,1,2},\cdots,\tilde{\Delta}_{j,1,k},\tilde{\Delta}_{j,2,1},\tilde{\Delta}_{j,2,2},\cdots,\tilde{\Delta}_{j,3,k})$$

其中 $\Delta_{j,x,y}$、$\tilde{\Delta}_{j,x,y}$,$(1\leqslant x\leqslant 3,1\leqslant y\leqslant k)$,与该标签第 x 种密码的第 y 个密码的更新有关,设该密码为 $\kappa_{x,y}$。由于密码更新时各个密码相互独立,可去除下标 x,y,则 $\kappa_{x,y}$ 用 κ 表示,$\Delta_{j,x,y}$、$\tilde{\Delta}_{j,x,y}$ 可用 $\Delta_{j,\kappa}$、$\tilde{\Delta}_{j,\kappa}$ 表示,$\Delta_{j,\kappa}$、$\tilde{\Delta}_{j,\kappa}$ 进一步分解为:

$$\Delta_{j,\kappa}=(\delta_{j,\kappa}^{(1)},\delta_{j,\kappa}^{(2)},\delta_{j,\kappa}^{(3)},\cdots,\delta_{j,\kappa}^{(m)}) \tag{1}$$
$$\tilde{\Delta}_{j,\kappa}=(\tilde{\delta}_{j,\kappa}^{(1)},\tilde{\delta}_{j,\kappa}^{(2)},\tilde{\delta}_{j,\kappa}^{(3)},\cdots,\tilde{\delta}_{j,\kappa}^{(m)})$$

设密码 κ 在第 j 次更新前的值为 κ_j。更新时先由式(2)更新 $\Delta_{j,\kappa}$,然后由式(3)更新 κ:

$$\begin{cases}\delta_{j+1,\kappa}^{(i)}=\delta_{j,\kappa}^{(i+1)}\oplus\tilde{\delta}_{j,\kappa}^{(i)},1\leqslant i\leqslant m-1\\ \delta_{j+1,\kappa}^{(m)}=\delta_{j,\kappa}^{(1)}\oplus\tilde{\delta}_{j,\kappa}^{(m)},i=m\end{cases} \tag{2}$$

$$\kappa_{j+1}=\kappa_j\oplus\delta_{j+1,\kappa}^{(1)} \tag{3}$$

其中⊕表示异或。式(2)相当于 $\Delta_{j,\kappa}$ 循环移位以后与 $\tilde{\Delta}_{j,\kappa}$ 相异或。

下面推导攻击者破解该协议的方法。由式(2)可得:

$$\delta_{j+1,\kappa}^{(1)}=\delta_{j,\kappa}^{(2)}\oplus\tilde{\delta}_{j,\kappa}^{(1)}=\delta_{j-1,\kappa}^{(3)}\oplus\tilde{\delta}_{j-1,\kappa}^{(2)}\oplus\tilde{\delta}_{j,\kappa}^{(1)}=\delta_{j-m+1,\kappa}^{(1)}\oplus\tilde{\delta}_{j-m+1,\kappa}^{(m)}\oplus\tilde{\delta}_{j-m+2,\kappa}^{(m-1)}\oplus\cdots\oplus\tilde{\delta}_{j,\kappa}^{(1)}=\delta_{j-m+1,\kappa}^{(1)}\oplus\sum_{i=1}^{m}\tilde{\delta}_{j-i+1,\kappa}^{(i)} \tag{4}$$

其中∑表示连续异或(本文默认情况下∑符号都为连续异或)。设密码 κ 在第 j 次和第 i 次交互$(j>i)$时的值为 κ_j 和 κ_i。则它们的关系由式(3)可得:

$$\kappa_j=\kappa_i\oplus\delta_{i+1,\kappa}^{(1)}\oplus\delta_{i+2,\kappa}^{(1)}\oplus\cdots\oplus\delta_{j,\kappa}^{(1)}=\kappa_i\oplus\sum_{x=1}^{j-i}\delta_{i+x,\kappa}^{(1)} \tag{5}$$

将式(4)代入式(5)可得:

$$\kappa_j=\kappa_i\oplus\sum_{x=1}^{j-i}(\delta_{i+x-m,\kappa}^{(1)}\oplus\sum_{y=1}^{m}\tilde{\delta}_{i+x-y,\kappa}^{(y)})$$
$$=\kappa_i\oplus\sum_{x=1}^{j-i}(\sum_{y=1}^{m}\tilde{\delta}_{i+x-y,\kappa}^{(y)})\oplus\sum_{x=1}^{j-i}(\delta_{i+x-m,\kappa}^{(1)}) \tag{6}$$

其中下标为正整数则要求 $i>m$。由式(5)可得式(6)中的

$$\sum_{x=1}^{j-i}\delta_{i+x-m,\kappa}^{(1)}=\kappa_{j-m}\oplus\kappa_{i-m} \tag{7}$$

将式(7)代入式(6)得

$$\kappa_j=\kappa_i\oplus\sum_{x=1}^{j-i}(\sum_{y=1}^{m}\tilde{\delta}_{i+x-y,\kappa}^{(y)})\oplus\kappa_{j-m}\oplus\kappa_{i-m} \tag{8}$$

令：

$$f_{\tilde{\delta}}(j,i)=\sum_{x=1}^{j-i}\left(\sum_{y=1}^{m}\tilde{\delta}_{i+x-y,\kappa}^{(y)}\right) \tag{9}$$

则式(8)变换为：

$$\begin{aligned}\kappa_j\oplus\kappa_i&=f_{\tilde{\delta}}(j,i)\oplus\kappa_{j-m}\oplus\kappa_{i-m}\\&=f_{\tilde{\delta}}(j,i)\oplus f_{\tilde{\delta}}(j-m,i-m)\oplus\kappa_{j-2m}\oplus\kappa_{i-2m}\\&=\left(\sum_{z=1}^{n}f_{\tilde{\delta}}(j-(z-1)m,i-(z-1)m)\right)\oplus\kappa_{j-nm}\oplus\kappa_{i-nm}\\&=\sum_{z=1}^{n}\left(\sum_{x=i+1-zm}^{j-zm}\left(\sum_{y=1}^{m}\tilde{\delta}_{x+m-y,\kappa}^{(y)}\right)\right)\oplus\kappa_{j-nm}\oplus\kappa_{i-nm}\end{aligned}$$

令：

$$g_m(x)=\sum_{y=1}^{m}\tilde{\delta}_{x+m-y,\kappa}^{(y)}$$

$$g_{\tilde{\delta}}(n,j,i)=\sum_{z=1}^{n}\left(\sum_{x=i+1-zm}^{j-zm}(g_m(x))\right) \tag{10}$$

则：

$$\kappa_j\oplus\kappa_i=g_{\tilde{\delta}}(n,j,i)\oplus\kappa_{j-nm}\oplus\kappa_{i-nm} \tag{11}$$

下标有意义，要求 $j>i>nm,n>0$。

式(10)和式(11)说明同一密码在不同交互时刻的密码值可通过 $\tilde{\delta}_{x,\kappa}^{(y)}$ 联系起来，也即通过 $\{\tilde{\Delta}_{x,\kappa},i-nm+1\leqslant x\leqslant j-1\}$ 联系起来。由于 $\tilde{\Delta}_{x,\kappa}$ 以明文传输，攻击者通过监听第 $i-nm+1$ 至 $j-1$ 次交互可获得 $\{\tilde{\Delta}_{x,\kappa},i-nm+1\leqslant x\leqslant j-1\}$。

设 d_j 为第 j 次交互时使用的密码序号。式(11)中的 κ 为同一个密码，为了通过监听获得 $\kappa_i,\kappa_{j-nm},\kappa_{i-nm}$ 且让第 j 次交互也使用 κ，必须要求：

$$d_j=d_i=d_{j-nm}=d_{i-nm} \tag{12}$$

且都等于 κ 的密码序号。式(12)称为式(11)的应用条件。由于最小限度算法的 d 每隔 k 次交互循环一次，这只要求：$i=j-k$，nm 为 k 的倍数即可。可以通过监听第 $j-k,j-nm,j-k-nm$ 次交互可获得 $\kappa_i,\kappa_{j-nm},\kappa_{i-nm}$。

综上，只要存在 $nm<i=j-k$，n 为正整数，nm 为 k 的倍数，攻击者通过监听第 $j-k-nm$ 至 $j-1$ 次交互可求得 κ_j。破解所需连续监听次数为 $k+nm$ 次。

2.3 最小限度算法的改进

$\tilde{\Delta}_{ABC}$ 以明文形式传输并可利用式(11)直接计算密码是该协议的弱点。改进方法着眼于破坏式(11)的成立条件以及信道加密来克服该弱点，共提出了 3 点改进方法。

3 实用的轻量级 RFID 安全协议

3.1 协议描述

改进后的协议如图 2 所示，有 3 个方面的改进：

1. d_j 不可直接计算。该改进使得式(11)的适用条件式(10)无法直接验证。实现方法是标签直接保存变量 d_j，并在每次交互后更新 d_j，更新方法是：

$$d_{j+1}=d_j\oplus\tilde{d}_j \tag{13}$$

其中 $\tilde{d}_j$ 是读写器产生的随机数，并传送给标签。此时 d_j 不再具有周期循环性，且若攻击者无法获知 $\tilde{d}_j$ 则 d_j 不可计算。

2. $\tilde{\Delta}_{j,\kappa}$ 不可直接计算。这使得式(11)中的 $g_{\tilde{\delta}}(n,j,i)$ 不可直接计算。设 S 是读写器产生的 3mk 比特的随机 bit 流，并发送给标签。$S(y)$ 为 S 的第 y 比特。设 $\hat{\Delta}_{ABC}$ 是读写器产生的 6mk 个 l 比特的随机数组成的 bit 流，并发送给标签。标签通过 S 选择 $\hat{\Delta}_{ABC}$ 中的随机数产生 $\tilde{\Delta}_{ABC}$。即若 $S(y)$ 等于 0，则 $\tilde{\Delta}_{ABC}$ 的第 y 个随机数选用 $\hat{\Delta}_{ABC}$ 的第 $2y-1$ 个随机数，否则选用 $\hat{\Delta}_{ABC}$ 的第 $2y$ 个随机数。当攻击者无法获得 S 时，$\tilde{\Delta}_{j,\kappa}$ 不可直接计算。

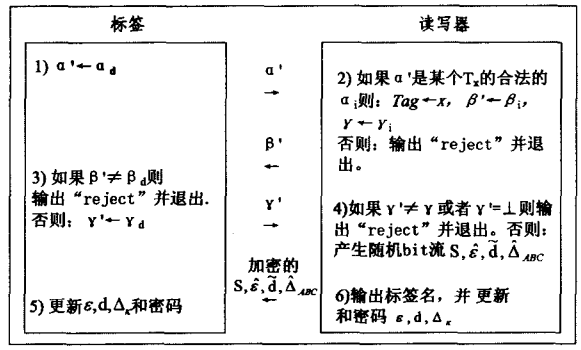

图 2 实用轻量级 RFID 安全协议

3. 信道加密。本文使用类似 One-time pad[12] 的方式加密信道。设一个 q 比特的信道密码 ε，标签和读写器共享 ε。命名图 2 第 4 步发送的数据流为：$F_j=S,\hat{\varepsilon},\tilde{d},\hat{\Delta}_{ABC}$ 发送时 F_j 需用 ε 加密，标签再通过 ε 解密。加密的方法是将 ε 和 F_j 相异或，如果 F_j 长于 ε 则重复使用 ε。设加密以后的 F_j 为 F_j'。为了提高安全性，信道密码 ε 在每次交互以后更新。设第 j 次更新前的信道密码为 ε_j，则更新方法为：

$$\varepsilon_{j+1}=\varepsilon_j\oplus\tilde{\varepsilon}_j \tag{14}$$

用 F_j 中的 $\hat{\varepsilon}$ 为索引在 $\hat{\Delta}_{ABC}$ 中提取 $\tilde{\varepsilon}_j$，即 $\tilde{\varepsilon}_j$ 是 $\hat{\Delta}_{ABC}$ 的第 $\hat{\varepsilon}$ 比特到 $\hat{\varepsilon}+q-1$ 比特的 bit 流。信道加密保证了 d_j 和 $\tilde{\Delta}_{j,\kappa}$ 不可直接计算。

3.2 改进效果分析

协议改进后，攻击者不可以使用式(11)直接求解 κ_j。改进后协议需增加的硬件支持主要有：

1)信道加密、更新 d_j、更新 ε_j 的异或操作。

2)使用 S 对 $\hat{\Delta}_{ABC}$ 进行选择，以 $\hat{\varepsilon}$ 为索引在 $\hat{\Delta}_{ABC}$ 中选取 $\tilde{\varepsilon}_j$。这些可以用计数器和简单的逻辑控制实现。

3)增加 q 比特信道密码存储单元。

可见改进协议增加的硬件资源不多，仍使用异或和简单的逻辑控制。

4 协议的计算机仿真

计算机仿真用于验证算法的可行性。

4.1 仿真思路

分别用两个程序模拟标签和读写器端的协议。标签和读写器的数据放置在各自的文件中。标签和读写器程序相互独立，没有隐含的数据交换。标签发给读写器的信息在屏幕上输出，用户将该输出信息输入到读写器程序窗口中，反之亦然，以此模拟两者的通信。

4.2 仿真结果

仿真程序时，取密码长度 l 为 16，密码个数 k 为 8，抗攻击强度 m 为 4，信道密码长度 q 为 16。共有标签 10 个，各个标签的数据存储在文件 0000 至 0010 文件中。

图 3 和图 4 分别为标签和读写器程序输入输出数据流(数据以十六进制表示)。图 3 中第一行，tag 0009 命令表示使用 0009 号标签。读写器经过和标签的数据交互以后识别

(下转第 118 页)

Computing, 2007. WiCom 2007, Wuhan, 2007
[6] Liang Wen-yau, Huang Chun-che, Chuang Horng-fu. The design with object (DwO) approach to Web services composition[J]. Computer Standards & Interfaces, 2007(29): 54-68
[7] Meng S, Arbab F. Web Services Choreograph and Orchestration in Reo and Constraint Automata[C]// AC'07. Seoul, Korea, March 2007
[8] Qiu Zongyan, Zhao Xiangpeng, Cai Chao, et al. Towards the Theoretical Foundation of Choreography[C]// IW3C2, 2007. Banff, Alberta, Canada, 2007
[9] Agarwal S, Handschuh S, Staab S. Annotation, composition and invocation of semanticweb services[J]. Web Semantics: Science, Services and Agents on the World Wide Web, 2004(2): 31-48
[10] Charif Y, Sabouret N. An Overview of Semantic Web Services Composition Approaches[J]. Electronic Notes in Theoretical Computer Science, 2006, 146: 33-41

(上接第 107 页)

标签名为 0009(如图 4 倒数第二行所示),说明识别正确。将该交互自动进行 1000 次,每次都能够识别正确。

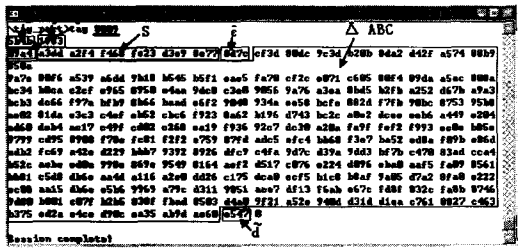

图 3 标签输入输出数据

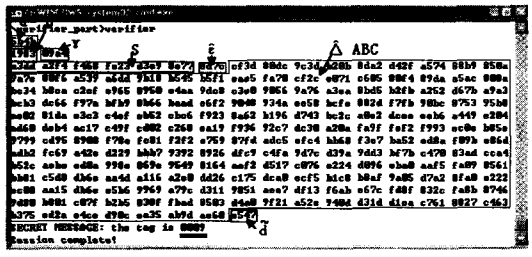

图 4 读写器输入输出数据

5 抗各种攻击的能力

本协议能够抗各种 RFID 中的常见攻击。

1. 跟踪:各次交互的 α',β',γ 和 F_j' 是动态变化的,根据式(3),攻击者只有获得 $\delta_{j,\kappa}^{(1)}$ 才知道密码值之间的关联性,$\delta_{j,\kappa}^{(1)}$ 不易获得。

2. 非法标签攻击,包括:

1)重放攻击:攻击者录制了标签发送给读写器的数据,并在以后伪装合法标签重放该数据。对本协议该攻击是无效的,因为一次成功交互以后的密码会更新,旧的密码值不再有效。

2)克隆标签:克隆标签发送的不正确的 α' 会被读写器拒绝。即使 α' 正确,也难以正确给出 γ。

3. 非法读写器攻击:非法读写器不能够就 α' 给出正确的 β',会被标签拒绝。

4. 非法读写器主动扫描标签信息:该攻击方法只能够获得当前 α',并不能够单独构成安全威胁。

结束语 在 RFID 安全的研究上,本文选择从第一类安全协议入手,该类协议只包含异或和简单的逻辑控制,非常适合在 RFID 上实现。本文在指出该类协议中的最小限度密码算法的弱点后,提出了 3 点改进方法。改进后的协议需通过强力攻击破解,克服了原协议能够根据交互数据直接计算密码值的缺点。实验结果表明,改进后的协议的破解需要更多的时间、更多的记录条数,同时改进后的协议对硬件需求的增加并不多。该研究成果将有助于在低成本的 RFID 芯片上实现较高安全性的 RFID 安全协议。

参 考 文 献

[1] Juels A. RFID Security and Privacy: A Research Survey[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 381-394
[2] 中华人民共和国科学技术部等十五部委. 中国射频识别(RFID)技术政策白皮书. 2006-06-09[OL]. http://www.eetchina.com/ARTICLES/2006JUN/PDF/CHINARFIDWHITEPAPER.PDF
[3] Feldhofer M, Dominikus S, Wolkerstorfer J. Strong Authentication for RFID Systems Using the AES Algorithm[C]// Cryptographic Hardware and Embedded Systems— CHES 2004—6th Int'l Workshop, LNCS 3156. Springer, 2004: 357-370
[4] Sarma S E, Weis S A, Engels D W. Radio-frequency-identification security risks and challenges[J]. CryptoBytes, 2003, 6(1)[OL]. http://www.rsasecurity.com/rsalabs/cryptobytes/CryptoBytes_March_2003_lowres.pdfJHJsearch=%22Radio-frequency-identification%20security%20risks%20and%20challenges%22
[5] Juels A, Pappu R. Squealing Euros: Privacy protection in RFIDenabled banknotes[C]// R. Wright, ed. Financial Cryptography '03, volume 2742 of Lecture Notes in Computer Science. Springer-Verlag, 2003: 103-121
[6] Sarma W S, Rivest R, Engels D. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems[C]// 1st Intern. Conference on Security in Pervasive Computing (SPC). 2003: 454-469
[7] Ohkubo M, Suzuki K, Kinoshita S. Cryptographic Approach to Privacy-friendly Tags[C]// RFID Privacy Workshop. MIT, 2003
[8] Avoine G, Oechslin P. A Scalable and Provably Secure Hash Based RFID Protocol[C]// the 2nd IEEE International Workshop on Pervasive Computing and Communication Security (PerSec), 2005[OL]. http://lasecwww.epfl.ch/pub/lasec/doc/AO05.pdfJHJsearch=%22filetype%3Apdf%20A%20Scalable%20and%20Provably%20Secure%20Hash%20Based%20RFID%20Protocol%22
[9] Dimitriou T. A Lightweight RFID protocol to protect against Traceability and Cloning attacks[C]// IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks, SECURECOMM 2005[OL]. http://www.ait.edu.gr/faculty/T_Dimitriou_files/RFID-securecomm05.pdfJHJsearch=%22filetype%3Apdf%20A%20Lightweight%20RFID%20protocol%20to%20protect%20against%20Traceability%20and%20Cloning%20attacks%22
[10] 周永彬,冯登国. RFID 安全协议的设计与分析[J]. 计算机学报, 2006, 29(04): 581-589
[11] Juels A. Minimalist Cryptography for Low-Cost RFID Tags[C]// Security in Communication Networks-Proc. 4th Int'l Conf., LNCS 3352. Springer, 2004: 149-164[OL]. http://www.rsasecurity.com/rsalabs/node.asp?id=2033
[12] Menezes A J, van Oorschot P C, Vanstone S A. Handbook of Applied Cryptography[M]. CRC Press, 1996: 21